REMARKS

The Examiner has objected to the Specification as failing to provide proper antecedent basis for the claimed subject matter. More specifically, the Examiner has argued that "the phrase 'computer readable medium,' appears to only reasonably convey hardware storage and forms of portable, physical article media to one of ordinary skill in the art." Applicant respectfully disagrees and notes that applicant specifically claims a "computer program product embodied on a tangible computer readable medium" (emphasis added), as claimed. Additionally, applicant notes that the term "tangible computer readable medium" is to be read according to the plain and ordinary meaning thereof, in view of dictionary definitions, and in further view of the definitions provided in the Specification.

In the Office Action mailed 11/06/2008, the Examiner has argued "the specification contains no definition of 'computer readable medium'" and has reiterated the argument that "the phase 'computer readable medium,' appears to only reasonably convey hardware storage and forms of portable, physical article media to one of ordinary skill in the art."

Applicant respectfully disagrees with such objection and points out that, for example, Paragraph [0050] of the Specification states that "[i]n operation the central processing unit 202 will execute computer program instructions that may be stored in one or more of the random access memory 204, the read only memory 206 and the hard disk drive 210 or dynamically downloaded via the network interface card 208" (emphasis added). Of course, such citations (in combination with the remaining specification) are merely examples of the above claim language and should not be construed as limiting in any manner.

Additionally, the Examiner has rejected Claims 1, 3-13, 15-18, 20-30, 32-35, 37-47, 49-52, and 55 under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. More specifically, the Examiner has argued that "[t]he

specification does not disclose how to detect whether the modified set of rules decreases malicious network traffic or slows malware propagation." Additionally, the Examiner has argued that "it is unclear how modified rules in one particular system has any effect on the amount of malicious traffic or the amount of propagated malware."

Applicant respectfully disagrees with such rejection and points out that, for example, Paragraph [0023] of the Specification states that "after a modified set [of rules] is transmitted to other computers some network sensors detect the effect (e.g., decrease of traffic) and send a 'positive' signal back" (emphasis added) and that this "raises the score or promotes a rule from 'temporary' into 'permanent' set." Of course, such citations (in combination with the remaining specification) are merely examples of applicant's claim language and should not be construed as limiting in any manner.

Additionally, the Examiner has rejected Claims 1, 3-13, 15-18, 20-30, 32-35, 37-47, 49-52, and 55 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Examiner has argued that "[t]he term 'more strongly associated' is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention."

Applicant respectfully disagrees with such rejection. In the Amendment filed 08/22/2007, applicant has respectfully asserted that such claim language is to be read according to the plain and ordinary meaning thereof, in view of dictionary definitions, etc. The Examiner, however, has argued that "it is uncertain what the association is stronger than." In response, applicant has respectfully asserted that the association is stronger than it would be without the modification of the set of rules.

In the Office Action mailed 11/01/2007, the Examiner has removed the rejection under 35 U.S.C. 112, second paragraph, but has responded to applicant's above arguments. In particular, the Examiner has argued that applicant's above arguments are

"not clear from the claim language," and that "it is not clear that the external program calls are more strongly associated with malicious computer program activity as compared to without the modifications." The Examiner has also argued that "[i]t could be more strongly associated with malicious computer program activity than the primary set of external program calls" such that "the scope of 'more strongly' cannot be ascertained."

Applicant respectfully disagrees. For example, with respect to the independent claims, applicant clearly claims "modifying said set of rules **such that** said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity" (see this or similar, but not necessarily identical language in the independent claims-emphasis added), as claimed. Therefore, it is clear that applicant's claimed "said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity" (emphasis added), as claimed, is definite.

In the Office Action mailed 07/17/2008, the Examiner has represented the rejection under 35 U.S.C. 112, second paragraph, and has argued that "[t]he term 'more strongly associated' in claims 1, 18, and 35 is a relative term which renders the claim indefinite" and has further argued that "[a]pplicant has failed to provide any actual rationale as to why the claims are definite."

Applicant respectfully disagrees. First, applicant again notes that the association of the "at least one secondary set of one or more external program calls" with "malicious computer program activity" is stronger than it would be without the modification of the set of rules, as claimed, which is clearly definite.

In the Office Action mailed 11/06/2008, the Examiner has stated that the applicant's "argument is not persuasive because the term 'more strongly associated' is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention."

Applicant respectfully disagrees and asserts that it is clear that applicant's claimed "said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity" (emphasis added), as claimed, is definite. Applicant again asserts that the association is stronger than it would be without the modification of the set of rules. Nevertheless, in the spirit of expediting the prosecution of the present application, applicant has clarified the independent claims as follows:

> "modifying said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity than said primary set of said one or more external program calls" (as amended – see this or similar, but not necessarily identical language in the aforementioned claims)

Therefore, it is clear that applicant's claimed "said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity than said primary set of said one or more external program calls" (emphasis added), as claimed, is definite.

Additionally, with respect to the Examiner's rejection of Claims 1, 3-13, 15-18, 20-30, 32-35, 37-47, 49-52, and 55 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention, the Examiner has argued that "it is unclear how modifying 'said set of rules' has any effect on a set of program calls that has already been logged, or the amount of malicious network traffic and malware propagation."

Applicant respectfully disagrees and asserts that applicant claims "modifying said set of **rules**," where "a primary set of one or more external program calls matching one or more **rules** indicative of malicious computer program activity from among a set of rules" is "identifiied] within said stream of external program calls" (see this or similar, but not

necessarily identical language in the independent claims-emphasis added), as claimed, which clearly shows the relationship between the "external program calls" and the "modifying," as claimed.

Further, applicant claims "**determining** whether said modified set of rules **decreases** malicious network traffic, and **promoting** said modified set of rules from a temporary set to a permanent set if it is determined that said modified set of rules decreases said malicious network traffic" (emphasis added), as claimed. Therefore, applicant's claimed "modifying said set of rules" has an effect on the amount of malicious network traffic since "if it is determined that said modified set of rules decreases said malicious network traffic," then "said modified set of rules [is promoted] from a temporary set to a permanent set" (emphasis added), as claimed. Therefore, applicant's claim language is clearly definite.

Additionally, with respect to the Examiner's rejection of Claims 1, 3-13, 15-18, 20-30, 32-35, 37-47, 49-52, and 55 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention, the Examiner has argued that "the term 'higher-level' in claim 55 is a relative term which renders the claim indefinite." Applicant respectfully asserts that such rejection has been avoided in view of the clarifications made hereinabove to Claim 55.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The

Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P489).

Respectfully submitted,
Zilka-Kotab, PC

/KEVINZILKA/

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100